Data Protection Policy

1 About the Data Protection Policy

1.1 Everyone has rights with regard to the way in which their Personal Data are handled. During the course of College Development Network's (the "organisation", "our", "we", "us") activities we will collect, store and process Personal Data about our customers, suppliers and other third parties. It is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

All data users are obliged to comply with this policy when processing Personal Data on the organisation's behalf, which includes all employees, workers, contractors and secondees. Consultants are obliged to adhere to this policy as part of their service agreement; contracting Managers are responsible for ensuring consultants' adherence. Any breach of this policy may result in disciplinary action. The UK Information Commissioner is the regulator that enforces Data Protection Laws in the UK and has powers to fine us up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of Data Protection Laws (defined in point 2, below).

1.2 The Director of Finance and Corporate Services is responsible for this policy. Please contact the Director of Finance and Corporate Services in the first instance for further information.

2 Policy Statement

The organisation aims to fulfil its obligations under the General Data Protection Regulation (EU) 2016/679, the Data Protection Act 2018 and all other applicable laws relating to the protection of Personal Data and privacy ("Data Protection Laws") to the fullest extent. Data Protection Laws states that the Personal Data we hold about Data Subjects must be:

1. Used lawfully, fairly and in a transparent way;
2. Collected only for valid purposes that the organisation has clearly explained to you and not used in any way that is incompatible with those purposes;
3. Relevant to the purposes the organisation has told you about and limited only to those purposes;
4. Accurate and kept up to date;
5. Kept only as long as necessary for the purposes the organisation has told you about;
6. Kept securely;
7. Not transferred to another country without appropriate safeguards being in place; and
8. Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data.

The organisation endorses fully, and adheres to, these principles of data protection, as set out in the Data Protection Laws.

This policy, and any other documents referred to in it, sets out the basis on which the organisation will process any Personal Data it collects from Data Subjects, or that is provided to it by Data Subjects or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy sets out rules on data protection and the legal conditions that must be satisfied when the organisation obtains, handles, processes, transfers and stores Personal Data[1].

[1] Note: For quick reference purposes you will find data protection dos and don'ts list at section 17 below. However, that list is not intended to summarise this policy and as such it should be read in addition to, and not instead of, this policy.

The Head of Marketing and Development is the organisation's named Data Protection Officer and is responsible for ensuring compliance with the Data Protection Laws and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Head of Marketing and Development.

Please contact the Head of Marketing and Development with any questions about the operation of this Data Protection Policy or the Data Protection Laws or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the Head of Marketing and Development in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the organisation);
(b) if you are unsure about the retention period for the Personal Data being Processed;
(c) if you are unsure about what security or other measures you need to implement to protect Personal Data;
(d) if there has been a Personal Data breach;
(e) if you are unsure on what basis to transfer Personal Data outside the EEA;
(f) if you need any assistance dealing with any rights invoked by a Data Subject;
(g) whenever you are engaging in a significant, new, or change in, Processing activity which is likely to require a Data Processing Impact Assessment (see section 15 below) or plan to use Personal Data for purposes others than what it was collected for;
(h) if you need help complying with applicable law when carrying out direct marketing activities; or
(i) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties.

3 UK Information Commissioner

The UK Information Commissioner is the independent regulator charged with policing and enforcing Data Protection Laws in the UK and with promoting good practice for compliance purposes.

The website of the UK Information Commissioner's Office (www.ico.org.uk) contains a wide range of useful information and guidance, both technical (legal) and practical, about the Data Protection Laws and what they require.

4 When Does Data Protection Legislation Apply?

The Data Protection Laws aim to ensure fairness, transparency and accountability in the "processing" of "Personal Data". It does so by requiring organisations which are "data controllers" to comply in their processing of Personal Data.

A "**data controller**" is any legal entity which determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the Data Protection Laws. The organisation is the data controller of all Personal Data relating to our company personnel and Personal Data used in our business for our own commercial purposes.

A "**Data Subject**" is living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

"**Personal Data**" are any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Category Personal Data and pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Please note that someone's work email address is also Personal Data.

"**Personal Data Breach**" any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

"**Special Category Personal Data**" information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions. The Data Protection Laws imposes certain additional requirements in respect of the processing of Special Category Personal Data in order to ensure that it is appropriately safeguarded. Members of staff should therefore always take particular care when dealing with Special Category Personal Data.

"**Processing**" (**inc Process, Processed etc.**) means holding or otherwise accessing or using Personal Data in any manner whatsoever; even simply reading it or telling someone about it. Essentially anything which staff do with Personal Data in the course of their work - including obtaining, holding, disclosing, using it and erasing/destroying it - is likely to amount to processing.

5 Lawfulness, Fairness and Transparency

5.1 Lawfulness and Fairness

Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

We may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The Data Protection Laws restrict our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The Data Protection Laws allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests; or

(e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

You must identify and document the legal basis being relied on for each Processing activity. One or more may apply at any one time. If in doubt, please speak to the Director of Finance and Corporate Services.

5.2 Transparency

Data Protection Laws require Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information will provided through our privacy notice.

Whenever we collect Personal Data directly from Data Subjects we must provide the Data Subject with all the information required by the Data Protection Laws.

When Personal Data are collected indirectly (for example, from a third party or publically available source), we must provide the Data Subject with all the information required by the Data Protection Laws as soon as possible after collecting/receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the Data Protection Laws and on a basis which contemplates our proposed Processing of that Personal Data.

6 Purpose

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have consented where necessary.

7 Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

We may only Process Personal Data when performing our job duties. You cannot Process Personal Data for any reason unrelated to your job duties.

We may only collect Personal Data that is required for our job duties. Do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

We must ensure that when Personal Data are no longer needed for specified purposes, it is deleted or anonymised in accordance with our data retention guidelines.

8 Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collect it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

9 Retention

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The organisation will maintain retention policies and procedures to ensure Personal Data are deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. Our key retention periods are detailed in our Records Retention and Disposal Policy.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with our Records Retention and Disposal Policy.

Please speak to the Director of Finance and Corporate Services before any non-routine deletion of Personal Data.

10 Data Security

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

Members of staff are responsible for ensuring that:

- any Personal Data they hold is kept securely and in accordance with the terms of our ICT Policy and our Personal Information and Security Policy;
- Personal Data are not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party;
- they comply with this Data Protection Policy.

Personal Data should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, the information must be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe. For further information on data and information security, please read our Personal Information and Security Policy.

Data should be held and disposed of in accordance with the terms of our Personal Information and Security Policy and our Document Retention and Disposal Policy.

11 Staff Members Personal Information

Members of staff are responsible for:

- checking that any information they provide to us in connection with their employment, secondment or consultancy services is accurate and up to date
- informing us of any changes to their personal information, for example changes of address, either at the time of appointment or thereafter.

12 Transferring Personal Data (to a country outside the EEA)

The organisation may transfer any Personal Data it holds to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- the Data Subject has provided explicit consent to the proposed transfer after being informed of any potential risks.
- the transfer is necessary for one of the reasons set out in the Data Protection Laws, including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent and in some limited cases, for our legitimate interest..
- the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms.
- appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism.

Subject to the requirements above, Personal Data we hold may also be processed by staff operating outside the EEA who work for the organisation or for one of its suppliers. That staff may be engaged in, among other things, the fulfilment of contracts with the Data Subject, the processing of payment details and the provision of support services.

13 Data Subjects and Subject Access Requests

Data Subjects have rights when it comes to how we handle their Personal Data.

These include rights to:

(a) withdraw consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data are transferred outside of the EEA;

(i) be notified of a Personal Data breach which is likely to result in high risk to their rights and freedoms;

(j) make a complaint to the supervisory authority; and

(k) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

It is important to first verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

Thereafter, it is important to immediately forward any Data Subject access request you receive to the Director of Finance and Corporate Services who will deal with the request in accordance with the Data Protection Laws.
If a Data Subject makes a formal request for information we hold about them under the Data Protection Laws such requests require us to respond to requests for access to Personal Data within 1 month of receipt.

Secondees
Secondees with the organisation are also required to adhere to this policy

Third Parties
Any member of staff who receives a written or telephoned subject access request should forward it to the Head of Marketing and Development immediately.

When receiving telephone enquiries, we will only disclose Personal Data it holds on its systems when the caller's identity has been checked to ensure they are entitled to the data.

We may suggest that a caller put their request in writing if their identity cannot be verified or checked.

All members of staff will refer a request to the Director of Finance and Corporate Services for assistance in difficult situations (members of staff should not be bullied into disclosing personal information).

14 Policy Breaches

If a member of staff thinks they may have breached this policy, they should speak to the Head of Marketing and Development immediately.

Quick action can be crucial in mitigating the negative effects of a breach, in particular where data security is concerned; it is therefore vital that members of staff raise the issue immediately in accordance with this policy.

It should be noted that failure to comply with this policy could constitute a disciplinary offence.

15 Data Breach

The Data Protection Laws requires us to notify any Personal Data Breach to the UK Information Commissioner and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Head of Marketing and Development. You should preserve all evidence relating to the potential Personal Data Breach.

It is important that you tell us if a Personal Data Breach has occurred. Even if the breach has been caused by you, please do not try to conceal it. Depending on the circumstances, in most cases it is our policy to treat such incidents as training issues rather than disciplinary issues.

16 Data Protection Impact Assessment

As a Data Controller, the organisation must conduct Data Protection Impact Assessments (DPIAs) in respect to high risk Processing.

You should conduct a DPIA (and discuss your findings with the Head of Marketing and Development) when implementing major system or business change programmes involving the Processing of Personal Data including:

(a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
(b) automated processing including profiling;
(c) large scale Processing of special category Personal Data; and
(d) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

(a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;
(c) an assessment of the risk to individuals; and
(d) the risk mitigation measures in place and demonstration of compliance.

17 Data Protection Dos and Don'ts

<u>Do</u>

- Do "think data protection" and “think privacy”. Members of staff should stop to think about whether what they are proposing to do works from a data protection and privacy compliance perspective.
- Do remember the two driving principles behind data protection:
  - fairness
  - transparency
- Do think very carefully before doing anything with Special Category Personal Data.
- Do check e-mail addresses carefully before sending an e-mail and do not just click through the external address pop-up screen checker.
- Do immediately bring to the attention of the Director of Finance and Corporate Services any subject access request which the organisation receives. A subject access request is a written request by or on behalf of any individual for a copy of any Personal Data which the organisation holds about that individual. There is no need for the person making the request to call it a "subject access request" or even to mention Data Protection Laws.

Do use common sense. The requirements of Data Protection Laws in many cases just reflect good data management practices and, as such, applying common sense is likely to be a good starting point in determining whether there will be an issue in a particular situation.

Don’t

- Do not access Personal Data held by the organisation in any form, unless access is reasonably required for work purposes.
- Do not commit to writing (whether email, a Word document, a handwritten note or otherwise) or otherwise record any opinions about any individual(s) unless:
  - it can be justified on reasonable grounds
  - there would be no issue with the individual in question in each case viewing what has been written about them.
- Do not take laptops, memory sticks or other portable IT devices storing Personal Data out of CDN's offices unless they are encrypted.
- Do not dispose of hard copies of information containing Personal Data anywhere other than in CDN's offices, using the confidential waste bins provided.

Do not disclose recipients' email addresses to all other recipients, when sending an email to more than one person, except if and to the extent that each recipient reasonably requires to have access to other recipients' email addresses, in light of the purpose and content of the email.